ABSTRACT

An apparatus for operating a cryptographic engine may include a key generation module for creating key pairs for encrypting substantive content to be shared between two users over a secured or unsecured communication link. The key generation module may include a point-modification module as part of an elliptic curve module for creating and processing keys. The point-modification module preferably employs a point-halving algorithm for creating and processing keys but may also employ any one or a combination of a variety of other algorithms. Hash functions may be used to further process ephemeral secrets or ephemeral keys that may be used for transactions, sessions, or other comparatively short time increments of communication. The keys generated by the key generation module may be configured to be processable by an encryption system for divulging independently to two independent parties a secret to be shared by the two independent parties. A point-halving algorithm may be provided to reduce the operation count of a cryptographic process.

Docket: 2944.2.1